

PŘEDMLUVA	9	5. SPRÁVA KLÍČŮ	153
1. ZÁKLADY KRYPTOGRAFIE	13	5.1 Životní cyklus klíčů	158
1.1 Základní pojmy	15	5.2 Transport klíčů	163
1.2 Kryptografické systémy	19	5.3 Délky klíčů	173
1.3 Teorie utajení a autentizace zpráv	25	6. KRYPTOGRAFIE V KOMUNIKAČNÍCH SYSTÉMECH	179
1.4 Matematika v kryptografii	34	6.1 Komunikační systémy s přepojováním okruhů	182
2. KRYPTOGRAFICKÉ FUNKCE A GENERÁTORY	49	6.1.1 Kryptografické zabezpečení spoje s časovým multiplexem	182
2.1 Jednosměrné funkce	51	6.1.2 Kryptografické zabezpečení sítě GSM	185
2.2 Generátory binárních posloupností	60	6.2 Komunikační systémy s přepojováním paketů	189
3. SYMETRICKÉ KRYPTOSYSTÉMY	69	6.2.1 Kryptografické zabezpečení v aplikační vrstvě	191
3.1 Proudové šifry	72	6.2.2 Kryptografické zabezpečení v transportní vrstvě	194
3.2 Blokové šifry	75	6.2.3 Kryptografické zabezpečení v síťové vrstvě	203
3.2.1 Bloková šifra AES	82	6.2.4 Kryptografické zabezpečení ve spojení vrstvě	210
3.2.2 Provozní režimy blokových šifer	89	7. DALŠÍ APLIKACE KRYPTOGRAFIE	217
3.3 Autentizace symetrickými kryptosystémy	100	7.1 Ochrana obsahu systémem AACCS	219
3.4 Dokonalá šifra a dokonalá autentizace	104	7.2 Autentizační protokol Kerberos	226
4. ASYMETRICKÉ KRYPTOSYSTÉMY	111	7.3 Platební protokol 3D Secure	230
4.1 Asymetrické kryptosystémy typu IF	113	DOSLOV	235
4.2 Asymetrické kryptosystémy typu DL	135	LITERATURA	237
4.3 Asymetrické kryptosystémy typu EC	144	SUMMARY	243
		REJSTŘÍK	245